



LA CONFIDENTIALITÉ DES DONNÉES

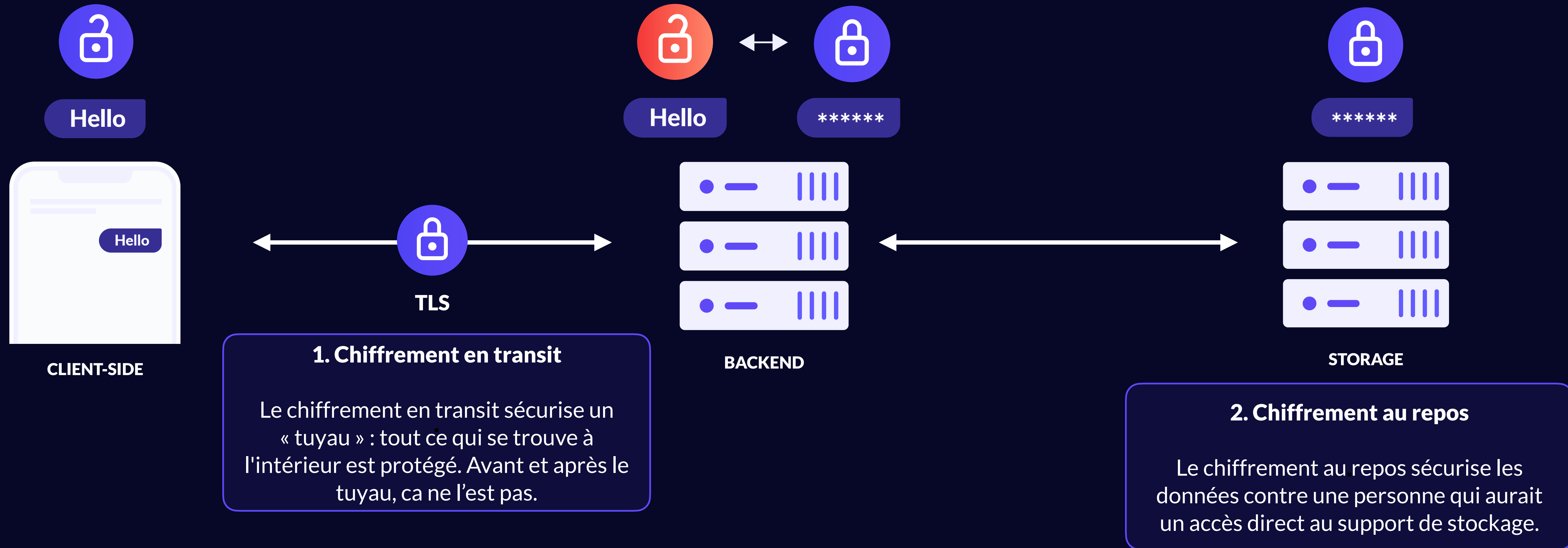
À L'ÉTAT DE L'ART

LES MÉTHODES CLASSIQUES

NE SUFFISENT PAS

3. Le backend peut lire les données

Si le backend peut lire les données, un hacker, un admin, une institution ou même un fournisseur de services peut également le faire.



SOLUTION: LE CHIFFREMENT

DE BOUT-EN-BOU

1. Chiffrement côté client

Le chiffrement est effectué avant l'envoi des données au backend.

2. Le backend ne peut pas lire les données

Le backend n'a plus accès aux données en clair. En cas d'accès non-autorisé à ce serveur, les données restent illisibles par l'attaquant. Cela est beaucoup plus strict que le chiffrement en transit combiné au chiffrement au repos.



POURQUOI LE CHIFFREMENT

DE BOUT-EN-BOUT ?

Confidentialité des données « par design »

Par exemple, les données chiffrées restent inaccessibles :

- En cas de fuite de données
- En cas d'un employé malveillant / trop curieux
- En cas d'attaque étatique

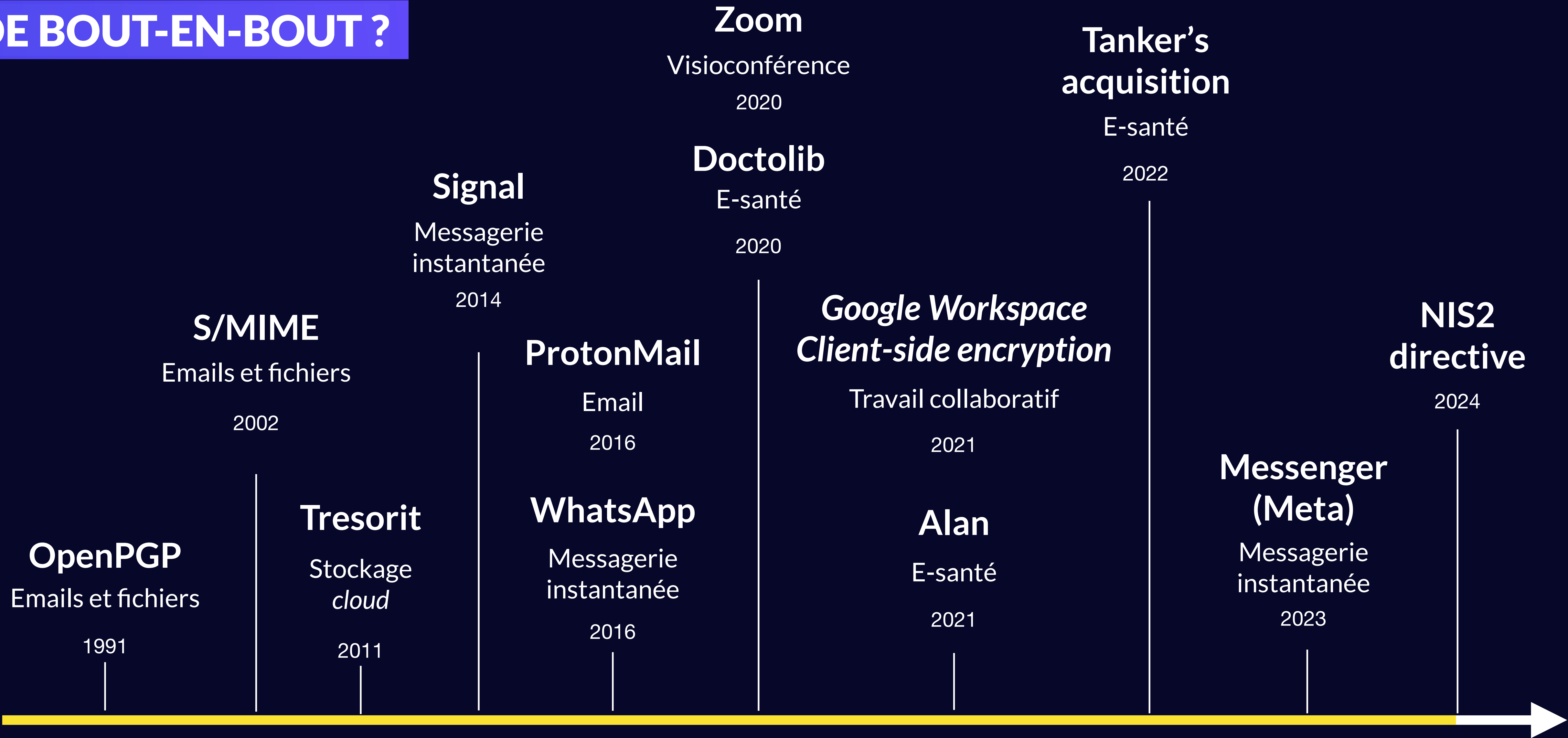
Respect de la réglementation

- RGPD: préconise du chiffrement, et selon plusieurs DPA le chiffrement peut être de bout-en-bout si les données sont très sensibles (données médicales par exemple)
- NIS2 : considérant 98 préconise explicitement du chiffrement de bout-en-bout
- Secret médical : les prestataires ne sont pas nécessairement habilités à lire les données

Réduire le risque du Cloud

- L'hébergeur ne peut plus lire les données, donc les prestataires de grands comptes encore réticents au cloud utilisent du E2EE pour les rassurer
- Protection contre les législations extra-territoriales

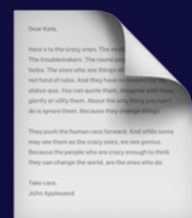
QUI UTILISE DU CHIFFREMENT DE BOUT-EN-BOUT ?



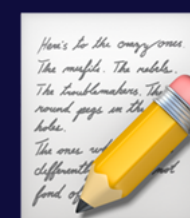
CAS D'USAGES



**Développeur
d'application**



**Stockage, partage de documents
et travail collaboratif**



Formulaire



Messagerie instantanée



**Données
juridiques**



**Données
médicales**



**Propriété
intellectuelle**



**Données
financières**

POURQUOI

SEALD



Le chiffrement de bout-en-bout est difficile à implémenter seul

Le chiffrement de bout-en-bout (ou chiffrement côté client) est **le plus haut niveau de sécurité** pour assurer la confidentialité des données, mais c'est aussi **le plus difficile et long à mettre en œuvre**. Souvent, les développeurs essaieront d'utiliser des bibliothèques open-source de bas niveau pour l'implémenter, difficiles à utiliser.

Lors de l'utilisation d'une telle bibliothèque, il faut encore choisir les primitives, une RNG robuste, implémenter un échange de clés publiques sécurisé, un mécanisme de récupération des clés privées, la gestion des groupes, la compatibilité multi-OS, etc.

Exemple : Meta a commencé son projet de chiffrement de bout-en-bout janvier 2019 et l'a terminé en décembre 2023.

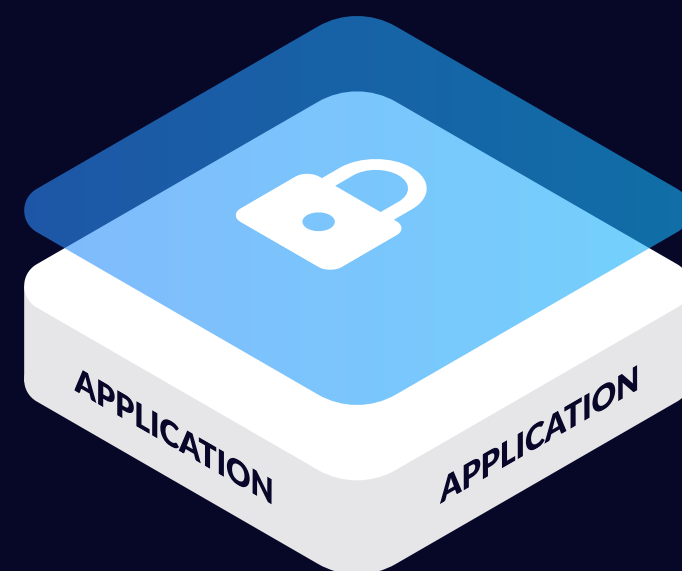
LA SOLUTION

SEALD



Un SDK de chiffrement de bout-en-bout certifié.

Le SDK Seald gère toute la complexité cryptographique et les échanges de clés pour vous.



Coming soon (2025):
Post-Quantum Cryptography

```
import SealdSDK from '@seald-io/sdk-web'

// Initialize the SDK
const seald = SealdSDK({ appId })
// Create your Seald identity
await seald.initiateIdentity({ userId: 'ALICE_001',
userLicenseToken })
// Encrypt a message for another user
const encryptedMessage = await seald.encryptMessage(
  'Super secret message',
  { userIds: ['BOB_002'] }
)

// And *voilà*!
const message = await seald.decryptMessage(encryptedMessage)
```



Browser JS



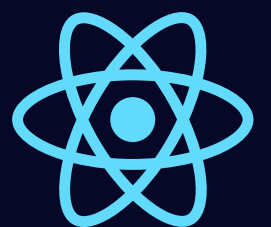
NodeJS



iOS

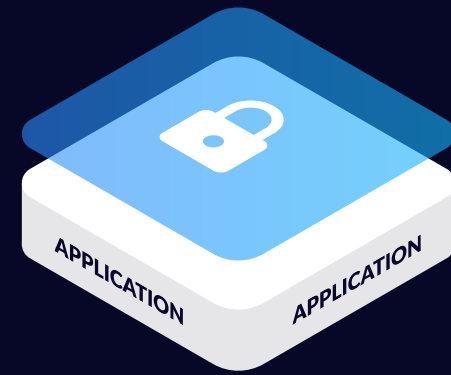


Android

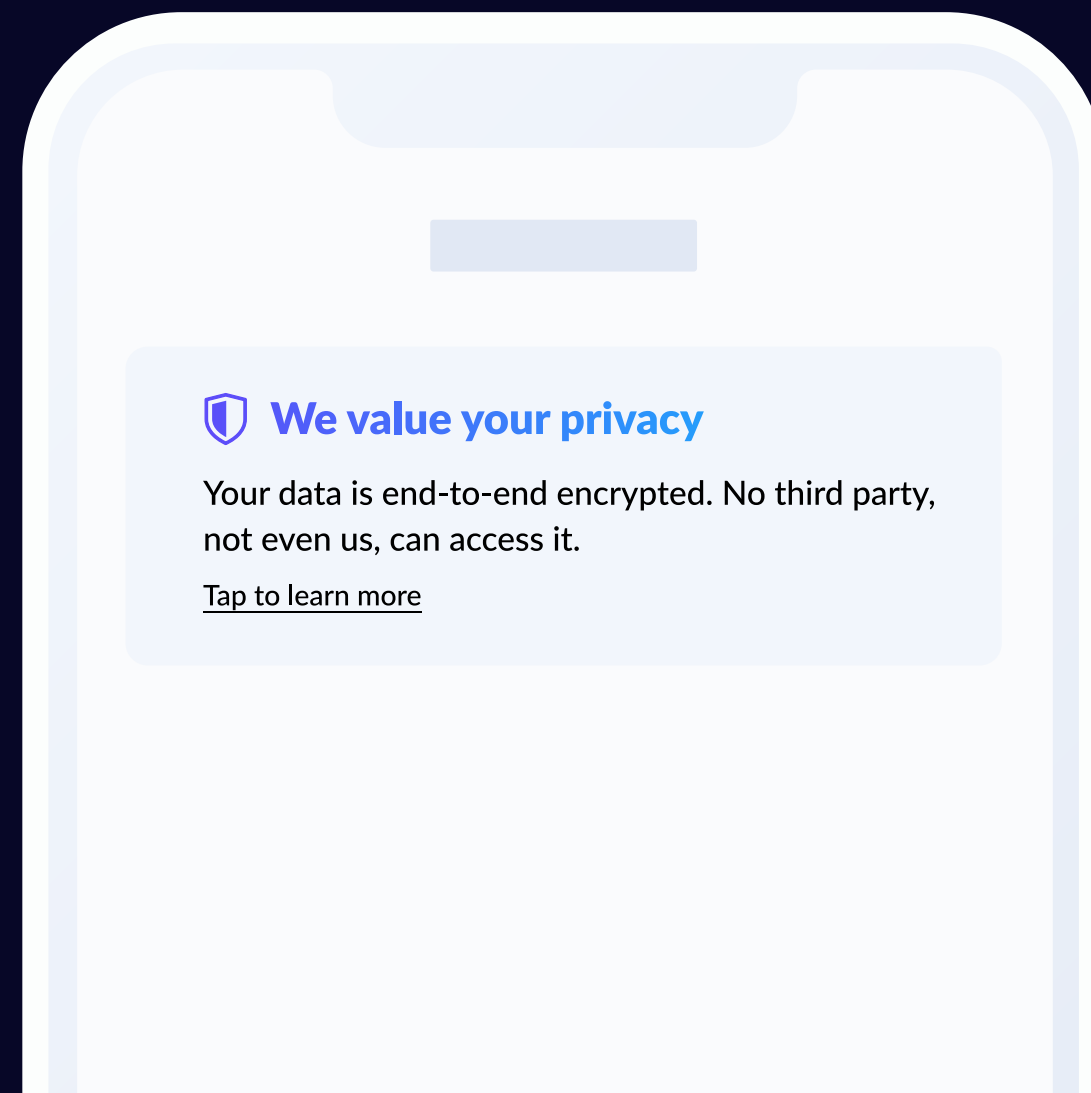


React Native

COMMENT ÇA MARCHE ?



Seald SDK

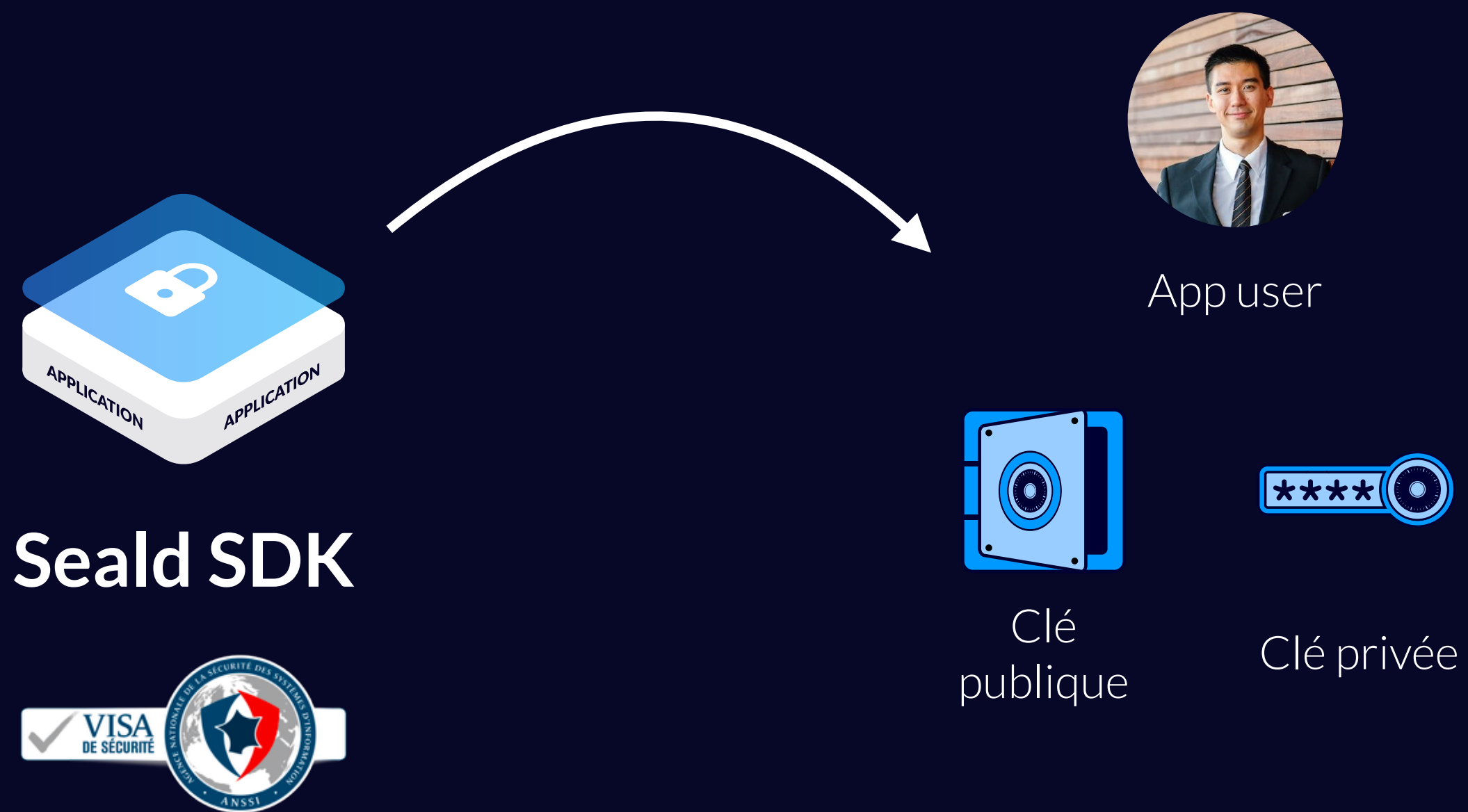


YOUR APP

Importez le Seald SDK dans l'app

Créez un compte Seald, récupérez vos clés API et importez le SDK dans votre application.

COMMENT ÇA MARCHE ?



Créez une paire de clés Seald pour chaque utilisateur

Générez une clé publique et une clé privée pour chaque utilisateur lors de la création de son compte. Publiez la clé publique sur les serveurs Seald. Récupérez la clé privée en toute sécurité lors de la connexion sur un nouvel appareil.

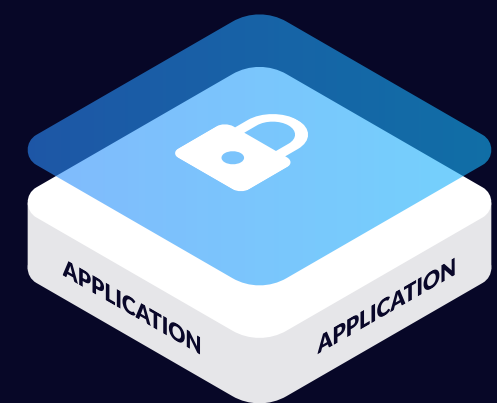
COMMENT ÇA MARCHE ?



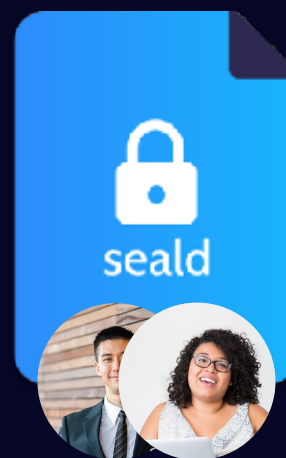
Utilisateurs
destinataires



Donnée en
clair



Seald SDK

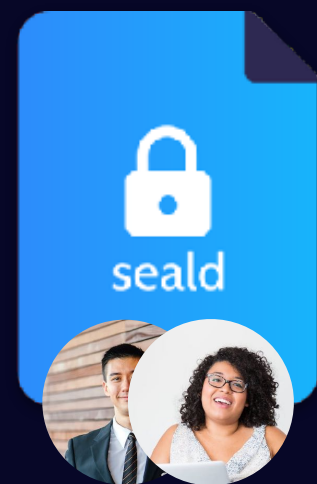


Donnée chiffrée
pour les utilisateurs
sélectionnées

Chiffrez les données pour les utilisateurs sélectionnées

Appelez la fonction `sdk.encrypt()` sur les données sensibles à protéger. Elles sont chiffrées côté client pour les seuls utilisateurs autorisés.

COMMENT ÇA MARCHE ?



Donnée chiffrée
pour les utilisateurs
sélectionnés



Your App Server

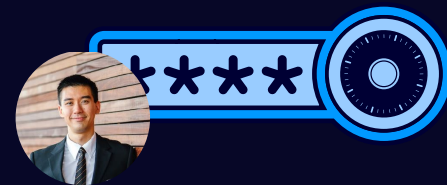
Envoyer les données chiffrées vers vos serveurs

Lorsque les données chiffrées sont reçues par vos serveurs, elles sont chiffrées avec une clé à laquelle vos serveurs n'ont jamais accès. En cas d'accès malveillant à vos serveurs, les données chiffrées sont à l'abri.

COMMENT ÇA MARCHE ?



Donnée chiffrée
pour les utilisateurs
sélectionnés



Clé privée



Seald SDK



Donnée en
clair

**Seuls les utilisateurs autorisés
peuvent déchiffrer les données.**

Les données chiffrées ne peuvent être déchiffrées
que par les utilisateurs autorisés. Pour ce faire,
un utilisateur utilise sa clé privée.

THEY TRUST

US

 Doktor.Se

 LPG
endermologie

 topboard

 recare

 STELLANTIS

 Hjemmelegene

 proximus

 Multipharma

 framatome

 BREDIN PRAT

 FRANCE
2030

 LEFEBVRE
SARRUT

 WIMI

 smartmerger

GARANTISSEZ LA CONFIDENTIALITÉ DES DONNÉES DANS LE CLOUD

“

La protection des données médicales est notre premier impératif. Nous avons décidé de remplacer notre technologie de chiffrement de bout-en-bout par Seald parce que leur technologie était supérieure du point de vue de la sécurité et de la fonctionnalité.



Charles Cote
CTO@Recare



www.seald.io

Follow us on:

